University of Louisiana at Lafayette

Information Technology Policy

Security and Acceptable Use Policies

Forward

1. IN ADDITION TO THE FOLLOWING POLICIES, THE UNIVERSITY OF LOUISIANA AT LAFAYETTE IS REQUIRED BY ACT 722 OF THE REGULAR LEGISLATURE OF 2001 TO ABIDE BY THE POLICIES AND STANDARDS AS PROMULGATED BY THE OFFICE OF INFORMATION TECHNOLOGY. (R.S. 39:15.1 ET SEQ. SEE:

2. *HTTP://WWW.STATE.LA.US/OIT/DOCS/STANDARDS_OVERVIEW.PDF*

3. *MUCH OF THIS DOCUMENT HAS BEEN ADAPTED FROM THE POLICIES OF THE SANS INSTITUTE 2006.*

Strategic Plan (Revised 5-09-2006)

Mission Statement for Information Technology

To provide, support and enhance computing and networking facilities which serve the academic and administrative needs of the University.

General Responsibilities of Computing and Networking Service Departments

- to provide, support and enhance campus computing and networking facilities, with emphasis on those which benefit multiple academic disciplines or administrative subunits;
- to establish policies and procedures which promote equitable access to computing for campus users and appropriate use of campus technology;
- to maintain the Information Technology infrastructure continuity plan;
- to respond to the needs and priorities of the administrative and support needs of faculty and student body of the University;
- to ensure the integrity and security of University's databases;
- to evaluate campus technology requirements and project future needs; and,
- to advise and/or assist members of the campus community in the use of whatever technology is appropriate for the accomplishment of their university-related activities.

Specific Current Responsibilities of Computing and Networking Service Departments

University Computing Support Services (UCSS)

- acquire, operate and support the facilities which provide basic online services (e-mail, browsing, file transfer, word processing, statistics, and other applications for general campus use; and program development environments for some degree programs);
- acquire, operate and support the campus web server and its emergency backup; assist with the production of official campus web pages; provide a server for the storage of personal web pages;
- acquire, operate and support the campus mail server and its MX alternate which provide direct access for users of Sun workstations, forwarding to alternate destination systems, and POP mail services for personal computers; provide a webmail server to allow access to campus email from any Internet browser;
- acquire, operate and support the campus Learning Management Server which now runs the Moodle LMS software;
- acquire, operate and support the campus NetReg and DHCP server which authorizes network access and provides IP addresses to authorized machines;
- acquire, operate and support the campus DNS servers which provide Internet name to address translation services;

- acquire, operate and support the campus portal hardware and database servers;
- allocate computing resources (accounts, disk space, file access) on the supported systems listed above;
- manage security and accountability for the use of the systems listed above;
- manage budgets for recurring computing costs (maintenance, leases, licenses, and supplies) for the systems above, and project future budget needs in these categories;
- request capital outlay funding (for new equipment) from the UL Lafayette administration and/or other sources, such as grants;
- document basic system features and train users in the basic operations of the supported systems listed above;
- advise and/or assist on-campus users (departments and/or individuals) with any computing tasks or problems they have, including (to the extent possible) with departmentally- or personally-owned PCs or Macs;
- assist the University or its subunits with acquisition procedures for computing software and hardware (evaluating products, developing specifications, negotiating contracts, site planning, obtaining State approvals, etc.), as appropriate.

Information Networks (IN)

- management, installation and repair of campus telephone/voice mail systems;
- management, installation and repair of campus data network;
- repair of university-owned PCs;
- support the campus modem pool;
- manage connectivity between the campus and the Internet (I1) and Internet 2 (I2);
- manage budgets for recurring communications costs (maintenance, leases, licenses, and supplies) for the systems above, and project future budget needs in these categories;
- request capital outlay funding (for new equipment) from the UL Lafayette administration and/or other sources, such as grants;
- interact with contracted and non-contracted vendors for materials parts and services required to maintain systems;
- work with architects, general contractors and electrical contractors to support networking in new building construction;
- work with physical plant to support networking in new building construction and building renovations and modification;
- enhancement of campus network bandwidth and reliability;
- oversee communications for the campus Emergency Operations Center;
- respond to Dottie (OneCall) requests locating and protecting underground services;
- respond to outages in University facilities, minimizing the impact to the campus;
- design, install and manage communications in the growing number of compressed video and smart classroom sites;

- manage telephone operator services for the campus;
- contract with various telephone companies for service;
- assist the University or its subunits with acquisition procedures for communications products (evaluating products, developing specifications, negotiating contracts, site planning, obtaining State approvals, etc.), as appropriate.

Office of Information Systems (OIS)

- manage and enhance software for administrative offices, especially any aspect of the administrative database (ISIS);
- train users in basic operations of the administrative database;
- advise and/or assist administrative offices with computing tasks or problems related to administrative software;
- acquire, operate and support the system which is used to provide an interface between the phone system and the IBM mainframe database;
- manage security and accountability in the use of administrative data;
- provide ID's and controlled access via authentication to University data bases;
- develop and manage the portal access to administrative and student data;
- produce special reports as required by the university administration or by the State.

Considerations in Continued Planning for Campus Needs

Academic planning

- evaluation and support of a campus-wide course content management system;
- evaluate and support access tools to improve student advising;
- provide faculty, staff, and students on-line access to all of their information with appropriate access controls;

- continue to provide ADA access and support for the needs of persons with disabilities;
- provide open access laboratories for students;
- develop tools for evaluating the effectiveness of the operation.

Administrative planning

- provide on-line processes for financial transactions for purchasing, time reporting, and other administrative activities.
- evaluate campus-wide printing and duplicating to determine the appropriate

balance between what is convenient and what is cost-effective;

- evaluate the policies for information retention in the administrative database with respect to (1) the funds required for additional disk space; and (2) the archival needs of the University;
- continue long-range planning and evaluation the hardware and software needs of the University;
- evaluate replacement equipment for the telephony and video needs of the campus;
- develop tools for evaluating the effectiveness of the operation

University of Louisiana at Lafayette Ethics Policy

1. **Overview**

   University of Louisiana at Lafayette purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every University of Louisiana at Lafayette employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

   University of Louisiana at Lafayette is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When University of Louisiana at Lafayette addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

   University of Louisiana at Lafayette will not tolerate any wrongdoing or impropriety at anytime. University of Louisiana at Lafayette will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. **Purpose**

   Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3. **Scope**

   This policy applies to employees, contractors, consultants, temporaries, and other workers at University of Louisiana at Lafayette, including all personnel affiliated with third parties.

4. **Policy**

   4.1. **Executive Commitment to Ethics**

   4.1.1. The Administration within University of Louisiana at Lafayette must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

   4.1.2. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

   4.1.3. Executives must disclose any conflict of interests regard their position within University of Louisiana at Lafayette.

   4.2. **Employee Commitment to Ethics**

   4.2.1. University of Louisiana at Lafayette employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

   4.2.2. Every employee needs to apply effort and intelligence in maintaining ethics value.

4.2.3. Employees must disclose any conflict of interests regard their position within University of Louisiana at Lafayette.

4.3. **Company Awareness**

4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2. University of Louisiana at Lafayette will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. **Maintaining Ethical Practices**

4.4.1. University of Louisiana at Lafayette will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2. Employees at University of Louisiana at Lafayette should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.5. **Unethical Behavior**

4.5.1. University of Louisiana at Lafayette will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2. University of Louisiana at Lafayette will not tolerate harassment or discrimination.

4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

4.5.4. University of Louisiana at Lafayette will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.5.5. University of Louisiana at Lafayette employees will not use corporate assets or business relationships for personal use or gain.

5. Enforcement

5.1. Any infractions of this code of ethics will not be tolerated and University of Louisiana at Lafayette will act quickly in correcting the issue if the ethical code is broken.

5.2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Acceptable Use Policy

1.0 Overview

Information Technology Security's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to University of Louisiana at Lafayette's established culture of openness, trust and integrity. Information Technology Security is committed to protecting University of Louisiana at Lafayette's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of University of Louisiana at Lafayette. These systems are to be used for business purposes in serving the interests of the university, and of our faculty, staff and students in the course of normal operations.

Effective security is a team effort involving the participation and support of every University of Louisiana at Lafayette employee, student and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at University of Louisiana at Lafayette. These rules are in place to protect the employees, students and University of Louisiana at Lafayette. Inappropriate use exposes University of Louisiana at Lafayette to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, other workers, and students at University of Louisiana at Lafayette, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased or under direct control of the University of Louisiana at Lafayette.

4.0 Policy

4.1 General Use and Ownership

1. While University of Louisiana at Lafayette's Information Technology Divisions desire to provide a reasonable level of privacy, users should be aware that the data they create on the university systems remains the property of University of Louisiana at Lafayette. Because of the need to protect University of Louisiana at Lafayette's network, management cannot guarantee the confidentiality of information stored on any device that is owned or leased or under direct control of the University of Louisiana at Lafayette.
2. Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees and students should consult the Office of Information Systems.

3. Information Technology Security recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Information Technology Security's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Information Technology Security's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within University of Louisiana at Lafayette may monitor equipment, systems and network traffic at any time, per Information Technology Security's Audit Policy.
5. University of Louisiana at Lafayette reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as public, internal or confidential as defined guidelines, details of which can be found in this series of documents. Examples of confidential information include but are not limited to: student information (grades, transcripts, enrollment, identification numbers, etc.) financial information, identification information of employees, and research data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed at least annually and user level passwords should be changed every four months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with the Office of Information Technology Security's Acceptable Encryption Use policy (IT Standard-023).
5. Because information contained on portable computers, PDA's and portable storage devices are especially vulnerable, special care should be exercised. Internal or private information must be encrypted. (IT-Policy-014).
6. Postings by employees from a University of Louisiana at Lafayette email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of University of Louisiana at Lafayette, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the University of Louisiana at Lafayette Internet/Intranet/Extranet, whether owned by the employee or University of Louisiana at Lafayette, shall be continually executing approved virus-scanning software with a current virus database.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of University of Louisiana at Lafayette authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing University of Louisiana at Lafayette-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by University of Louisiana at Lafayette.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which University of Louisiana at Lafayette or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a University of Louisiana at Lafayette computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any University of Louisiana at Lafayette account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Information Technology Security is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, University of Louisiana at Lafayette employees to parties outside University of Louisiana at Lafayette.
16. Providing data or other information that is not public to any outside entity without approval is prohibited.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within University of Louisiana at Lafayette's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by University of Louisiana at Lafayette or connected via University of Louisiana at Lafayette's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all University of Louisiana at Lafayette employees and affiliates.

3.0 Policy (See OIT STD 023)

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. University of Louisiana at Lafayette’s key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Information Technology Security. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Application Service Providers (ASP) Policy

1.0 Purpose

This document describes Information Security's requirements of Application Service Providers (ASPs) that engage with University of Louisiana at Lafayette.

2.0 Scope

This policy applies to any use of Application Service Providers by University of Louisiana at Lafayette, independent of where hosted.

3.0 Policy

3.1 Requirements of Project Sponsoring Division

The ASP Sponsoring Division must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within University of Louisiana at Lafayette or ASPs external to the company. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this policy. The Business Function to be outsourced must be evaluated against the following:

1. The requester must go through the ASP engagement process with the ASP Tiger Team to ensure affected parties are properly engaged.
2. In the event that University of Louisiana at Lafayette data or applications are to be manipulated by, or hosted at, an ASP's service, the ASP sponsoring division must have written, explicit permission from the data/application owners. A copy of this permission must be provided to Information Technology Security.
3. The information to be hosted by an ASP must fall under the "Minimal" or "More Sensitive" categories. Information that falls under the "Most Sensitive" category may not be outsourced to an ASP. Refer to the *Information Sensitivity Policy* for additional details.
4. If the ASP provides confidential information to University of Louisiana at Lafayette, the ASP sponsoring division is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. University of Louisiana at Lafayette's legal services department should be contacted for further guidance if questions about third-party data arise. Projects that do not meet these criteria may not be deployed to an ASP.

3.2 Requirements of the Application Service Provider

Information Technology Security has created an associated document, entitled *ASP Security Standards* that sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use.

The ASP engagement process includes an Information Technology Security evaluation of security requirements. The *ASP Security Standards* can be provided to ASPs that are either being considered for use by University of Louisiana at Lafayette, or have already been selected for use.

Information Technology Security may request that additional security measures be implemented in addition to the measures stated in the *ASP Security Standards* document, depending on the nature of the project. Information Technology Security may change the requirements over time, and the ASP is expected to comply with these changes.

ASPs that do not meet these requirements may not be used for University of Louisiana at Lafayette projects.

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment. Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	**Definitions**
Application Service Provider (ASP)	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a University of Louisiana at Lafayette-owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.
ASP Sponsoring Division	The group within University of Louisiana at Lafayette that wishes to utilize the services of an ASP.
Business Function	The business need that a software application satisfies. managed by an ASP that hosts an application on behalf of University of Louisiana at Lafayette.

6.0 Revision History

ASP Security Standards

1.0 Overview

This document defines the minimum security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by University of Louisiana at Lafayette. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. Information Technology Security (IT-SEC) will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. (IT-SEC) approval of any given ASP resides largely on the vendor's response to this document.

These Standards are subject to additions and changes without warning by IT-SEC.

2.0 Scope

This document can be provided to ASPs that are either being considered for use by University of Louisiana at Lafayette, or have already been selected for use.

3.0 Responding to These Standards

IT-SEC is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, e.g.:

Examples:

Bad: "We have hardened our hosts against attack."
Good: "We have applied all security patches for Windows 2000 as of 8/31/2000 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to University of Louisiana at Lafayette."

Bad: "We use encryption."
Good: "All communications between our site and University of Louisiana at Lafayette will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

4.0 Standards

4.1 General Security

1. University of Louisiana at Lafayette reserves the right to periodically audit the University of Louisiana at Lafayette application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (basic portscans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.

2. The ASP must provide a proposed architecture document that includes a full network diagram of the University of Louisiana at Lafayette Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where University of Louisiana at Lafayette data resides, the applications that manipulate it, and the security thereof.

3. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

4.2 Physical Security

1. The equipment hosting the application for University of Louisiana at Lafayette must be located in a physically secure facility, which requires badge access at a minimum.

2. The infrastructure (hosts, network equipment, etc.) hosting the University of Louisiana at Lafayette application must be located in a locked cage-type environment.

3. University of Louisiana at Lafayette shall have final say on who is authorized to enter any locked physical environment, as well as access the University of Louisiana at Lafayette Application Infrastructure.

4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for University of Louisiana at Lafayette.

5. University of Louisiana at Lafayette's Corporate Asset Protection team requires that the ASP disclose their ASP background check procedures and results prior to IT-SEC granting approval for use of an ASP.

4.3 Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the University of Louisiana at Lafayette application environment must use separate hosts, and separate infrastructure.

2. How will data go between University of Louisiana at Lafayette and the ASP? Keep in mind the following two things:

   a. If University of Louisiana at Lafayette will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the University of Louisiana at Lafayette extranet, and the operation of that circuit will come under the procedures and policies that govern the University of Louisiana at Lafayette Partner Network Management Group.

b. If, on the other hand, the data between University of Louisiana at Lafayette and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between University of Louisiana at Lafayette and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, NT, etc.) comprising the University of Louisiana at Lafayette application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.

2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

3. Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?

4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.

5. The ASP must provide information on their password policy for the University of Louisiana at Lafayette application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

6. University of Louisiana at Lafayette cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

7. The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

4.5 Web Security

1. At University of Louisiana at Lafayette's discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or ASP (active server page) technology.

3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

5. Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

4.6 Cryptography

1. The University of Louisiana at Lafayette application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the University of Louisiana at Lafayette application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

2. Encryption algorithms must be of sufficient strength to equate to 168-bit TripleDES.

3. Preferred hashing functions are SHA-1 and MD-5.

4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.

5. If the University of Louisiana at Lafayette application infrastructure requires PKI, please contact University of Louisiana at Lafayette Information Security Group for additional guidance.

DB Password Policy

1.0 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of University of Louisiana at Lafayette's networks.

Computer programs running on University of Louisiana at Lafayette's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2.0 Scope

This policy applies to all software that will access a University of Louisiana at Lafayette, multi-user production database.

3.0 Policy

3.1 General

In order to maintain the security of University of Louisiana at Lafayette's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2 Specific Requirements

3.2.1. Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

3.2.2. Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4. Coding Techniques for implementing this policy

[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or C pro.]

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.

Executing body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

6.0 Revision History

Computing Facility Security Policy

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in University of Louisiana at Lafayette Computing Facilities (here after known as Facility or Facilities) located on the "PUBLIC SERVICE VLAN or INTERNAL UNSECURE VLAN or De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to University of Louisiana at Lafayette from the damage to public image caused by unauthorized use of University of Louisiana at Lafayette resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope

University of Louisiana at Lafayette facility networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located on the PUBLIC SERVICE VLAN or INTERNAL UNSECURE VLAN and are subject to this policy. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents.

3.0 Policy

3.1. Ownership and Responsibilities

1. All facilities covered by this policy must present a University mission justification with sign-off at the Vice President level. Information Technology Security must keep the business justifications on file.
2. Facility owning organizations are responsible for assigning facility managers, point of contact (POC), and back up POC, for each facility. The facilitiy owners must maintain up to date POC information with Information Technology Security. Facility managers or their backup must be available around-the-clock for emergencies by an immediate electronic contact method.
3. Changes to the connectivity and/or purpose of existing facilities and establishment of new DMZ Labs must be requested through and approved by Information Technology Security.
4. All network connections must be maintained by a Information Networks.
5. Information Networks must maintain a firewall device between the facility, the remainder of the non-public campus network and the Internet.
6. Information Networks and Information Technology Security may interrupt lab connections if a security concern exists.
7. The facility will provide and maintain network devices deployed up to the Information Networks' point of demarcation.
8. The Information Networks must manage and maintain all IP address space.

9. The facility managers are ultimately responsible for their facilities complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of Information Technology Security and the Information Networks upon request, in accordance with the *Audit Policy*
11. Individual lab accounts which provide access to facilities must be deleted within three (3) days when access is no longer authorized. Group accounts are not permitted.
12. Information Technology Security will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. University mission critical resources must not depend upon resources not managed by the Information Technology Division.
2. Facilities not managed by the Information Technology Division must not be connected to University of Louisiana at Lafayette's internal or confidential networks, either directly or via a wireless connection.
3. Facilities not managed by the Information Technology Division should be in a physically separate room from any internal or internal secure network ports. When this is not possible, access to the facility hardware will be limited as directed by Information Technology Security.
4. Lab Managers are responsible for complying with the following related policies:
   a. *Password Policy*
   b. *Wireless Communications Policy*
   c. *Lab Anti-Virus Policy*
5. The Information Networks maintained firewall devices must be configured in accordance with least-access principles and the University mission needs. All firewall filters will be approved by Information Technology Security and implemented by Information Networks.
6. The firewall device must be the only access point between the Public Access Facilities and the rest of University of Louisiana at Lafayette's networks and other external networks. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes must be reviewed and approved by Information Technology Security (including both general configurations and rule sets). Information Technology Security may require additional security measures as needed.
8. Traffic from facilities to the University of Louisiana at Lafayette internal network, including VPN access, falls under the *Remote Access Policy*.
9. All routers and switches not used for testing and/or training must conform to the facilities standardization documents.
10. Operating systems of all hosts internal to the facilities running Internet Services must be configured to the secure host installation and configuration standards.
11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.

12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
13. Services and applications not serving mission of the University must be disabled.
14. University of Louisiana at Lafayette's internal and confidential information is prohibited on equipment in facilities not managed by the Information Technology Division where non-University of Louisiana at Lafayette personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*.
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the normal facility networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
DMZ (de-militarized zone)	Networking that exists outside of University of Louisiana at Lafayette primary corporate firewalls, but is still under University of Louisiana at Lafayette administrative control.
Network Support Organization	Any Information Technology Security-approved support organization that manages the networking of non-lab networks.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
Network Support Organization Point of Demarcation	The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.

Lab Manager

The individual responsible for all lab activities and personnel.

Lab

A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

Firewall

A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by Information Technology Security.

Internally Connected Lab

A lab within University of Louisiana at Lafayette's corporate firewall and connected to the corporate production network.

6.0 Revision History

University of Louisiana at Lafayette Email Use Policy

1.0 Purpose

To prevent tarnishing the public image of University of Louisiana at Lafayette When email goes out from University of Louisiana at Lafayette the general public will tend to view that message as an official policy statement from the University of Louisiana at Lafayette.

2.0 Scope

This policy covers appropriate use of any email sent from a University of Louisiana at Lafayette email address and applies to all employees, vendors, and agents operating on behalf of University of Louisiana at Lafayette.

3.0 Policy

3.1 Prohibited Use. The University of Louisiana at Lafayette email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any University of Louisiana at Lafayette employee should report the matter to their supervisor immediately.

3.2 Personal Use.

Using a reasonable amount of University of Louisiana at Lafayette resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a University of Louisiana at Lafayette email account is prohibited. Virus or other malware warnings and mass mailings from University of Louisiana at Lafayette shall be approved by University of Louisiana at Lafayette VP Information Technology before sending. These restrictions also apply to the forwarding of mail received by a University of Louisiana at Lafayette employee.

3.3 Monitoring

University of Louisiana at Lafayette employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system. University of Louisiana at Lafayette may monitor messages without prior notice. University of Louisiana at Lafayette is not obliged to monitor email messages.

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.

Chain email or letter Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information Information is considered sensitive if it can be damaging to University of Louisiana at Lafayette or its customers' reputation or market standing.

Virus warning. Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

Unauthorized Disclosure The intentional or unintentional revealing of restricted information to people, both inside and outside University of Louisiana at Lafayette, who do not have a need to know that information.

6.0 Revision History

Extranet Policy

1.0 Purpose

This document describes the policy under which third party organizations connect to University of Louisiana at Lafayette networks for the purpose of transacting business related to University of Louisiana at Lafayette.

2.0 Scope

Connections between third parties that require access to non-public University of Louisiana at Lafayette resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for University of Louisiana at Lafayette or to the Public Switched Telephone Network does NOT fall under this policy.

3.0 Policy

3.1 Pre-Requisites

3.1.1 Security Review

All new extranet connectivity will go through a security review with the Information Security department (Information Technology Security). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

3.1.2 Third Party Connection Agreement

All new connection requests between third parties and University of Louisiana at Lafayette require that the third party and University of Louisiana at Lafayette representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by the Vice President of the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into University of Louisiana at Lafayette labs are to be kept on file with the [name of team responsible for security of labs].

3.1.3 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the [name of team responsible for security of labs]. Typically this function is handled as part of the *Third Party Agreement*.

3.1.4 Point Of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the *Third Party Agreement* that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

3.2 Establishing Connectivity

Sponsoring Organizations within University of Louisiana at Lafayette that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage Information Technology Security to address security issues inherent in the project. If the proposed connection is to terminate within a lab at University of Louisiana at Lafayette, the Sponsoring Organization must engage the [name of team responsible for security of labs]. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and Information Technology Security, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will University of Louisiana at Lafayette rely upon the third party to protect University of Louisiana at Lafayette's network or resources.

3.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or Information Technology Security when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within University of Louisiana at Lafayette must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct University of Louisiana at Lafayette business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct University of Louisiana at Lafayette business necessitate a modification of existing permissions, or termination of connectivity, Information Technology Security and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**

Circuit
For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.

Sponsoring Organization
The University of Louisiana at Lafayette organization who requested that the third party have access into University of Louisiana at Lafayette.

Third Party
A business that is not a formal or subsidiary part of University of Louisiana at Lafayette.

6.0 Revision History

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of University of Louisiana at Lafayette without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect University of Louisiana at Lafayette Confidential information (e.g., University of Louisiana at Lafayette Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to VP Information Technology.

2.0 Scope

All University of Louisiana at Lafayette information is categorized into three main classifications:

- University of Louisiana at Lafayette Public
- University of Louisiana at Lafayette Internal (a.k.a. University)
- University of Louisiana at Lafayette Confidential

University of Louisiana at Lafayette Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to University of Louisiana at Lafayette.

University of Louisiana at Lafayette Internal Information is data that has not been declared public, is not structured or formatted for the public, and should not be released to the public. However, release of these data would not cause damage to the University.

University of Louisiana at Lafayette Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, individual student information, individual personnel information, medical information, social security identification, etc.. Also included in University of Louisiana at Lafayette Confidential is information that is less critical, such as telephone directories, and email lists.

A subset of University of Louisiana at Lafayette Confidential information is "University of Louisiana at Lafayette Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to University of Louisiana at Lafayette by that company under non-disclosure agreements and other contracts. Examples of this type of information include research findings, proprietary software, etc.

University of Louisiana at Lafayette personnel is encouraged to use common sense judgment in securing University of Louisiana at Lafayette Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as University of Louisiana at Lafayette Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the University of Louisiana at Lafayette Confidential information in question.

3.1 **Minimal Sensitivity:** General University information; some personnel and technical information

Requests for all public or internal information must be directed to the Institutional Research Office (IRES) for compilation and distribution. IRES is responsible for the coordination and completion of all external surveys, questionnaires and mandated governmental reporting about UL Lafayette. IRES also provides semester and longitudinal reports to members of the university community. The Registrar's Office is responsible for providing official transcripts. News Services is responsible for providing information regarding activities on campus and coordinating information to news media.

Access: University of Louisiana at Lafayette employees, contractors, people with a business need to know.
Distribution within University of Louisiana at Lafayette: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of University of Louisiana at Lafayette internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on University of Louisiana at Lafayette premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **Most Sensitive:** Examples include: Educational records of students covered by the Family Educational Rights and Privacy Act of 1974, medical information covered by HIPII, personal information covered by the Act No. 499 (Louisiana Senate Bill 205 enrolled in the 2005 Regular Session) protecting individual's name when associated with any of the following: social security number, driver's license number, account number when associated with credit or debit card number that would permit access to an individual's financial account, and medical information.

Access: Only those individuals (University of Louisiana at Lafayette employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within University of Louisiana at Lafayette: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of University of Louisiana at Lafayette internal mail: Delivered direct; signature required; approved private carriers.
Data stored on notebooks PC's, PDA's or Portable Storage Devices: All sensitive data that is stored on University approved portable storage devices (Notebook PC's, USB thumb drives, USB hard drives, CD's, DVD's, diskettes, PDA's, etc.) that are removed from the premises must be encrypted and consistent with OIT STD 023 (Encryption Standard.)

Electronic distribution: There are no restrictions to approved recipients within University of Louisiana at Lafayette, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on University of Louisiana at Lafayette premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Configuration of University of Louisiana at Lafayette-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by the University Computing Support Services. These include, but are not necessarily limited to, Outlook, Open Webmail, Microsoft Outlook Express, Mac OS X Mail, UCS Telnet Session (access to email via Elm).

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac’s and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of University of Louisiana at Lafayette.

Encryption
Secure University of Louisiana at Lafayette sensitive information in accordance with the Acceptable Encryption Policy (OIT STD 023). International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to University of Louisiana at Lafayette's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

6.0 Revision History

Internal Lab Security Policy

1.0 Purpose

This policy establishes information security requirements for University of Louisiana at Lafayette labs to ensure that University of Louisiana at Lafayette confidential information and technologies are not compromised, and that production services and other University of Louisiana at Lafayette interests are protected from lab activities.

2.0 Scope

This policy applies to all internally connected labs, University of Louisiana at Lafayette employees and third parties who access University of Louisiana at Lafayette's labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities

1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with Information Technology Security and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard University of Louisiana at Lafayette from security vulnerabilities.

3. Lab managers are responsible for the lab's compliance with all University of Louisiana at Lafayette security policies. The following are particularly important: *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.

4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

6. The Network Support Organization and/or Information Technology Security reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The Network Support Organization must record all lab IP addresses, which are routed within University of Louisiana at Lafayette networks, in Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to Information Technology Security with business justification, the equipment, and the IP address space information. Information Technology Security will review for security concerns and must approve before such connections are implemented.

9. All user passwords must comply with University of Louisiana at Lafayette's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains University of Louisiana at Lafayette proprietary information, group account passwords must be changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. Information Technology Security will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by Information Technology Security. Information Technology Security may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-University of Louisiana at Lafayette networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. Information Technology Security reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all University of Louisiana at Lafayette product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with University of Louisiana at Lafayette's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-University of Louisiana at Lafayette personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no University of Louisiana at Lafayette confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by Information Technology Security.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy*.

10. All lab external connection requests must be reviewed and approved by Information Technology Security. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to University of Louisiana at Lafayette corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from Information Technology Security is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Internal — A lab that is within University of Louisiana at Lafayette's corporate firewall and connected to University of Louisiana at Lafayette's corporate production network

Network Support Organization — Any Information Technology Security approved University of Louisiana at Lafayette support organization that manages the networking of non-lab networks.

Lab Manager -
The individual responsible for all lab activities and personnel

Lab
A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

External Connections (also known as DMZ)
External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.

Lab Owned Gateway Device
A lab owned gateway device is the lab device that connects the lab network to the rest of University of Louisiana at Lafayette network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by Information Technology Security.

Telco
A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.

Traffic
Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.

Firewall
A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by Information Technology Security.

Extranet
Connections between third parties that require access to connections non-public University of Louisiana at Lafayette resources, as defined in Information Technology Security's Extranet policy (link).

DMZ (De-Militarized Zone)
This describes network that exists outside of primary corporate firewalls, but are still under University of Louisiana at Lafayette administrative control.

6.0 Revision History

Internet DMZ Equipment Policy

1.0 Purpose

The purpose of this policy is to define standards to be met by all equipment owned and/or operated by University of Louisiana at Lafayette located outside University of Louisiana at Lafayette's corporate Internet firewalls. These standards are designed to minimize the potential exposure to University of Louisiana at Lafayette from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of University of Louisiana at Lafayette resources.

Devices that are Internet facing and outside the University of Louisiana at Lafayette firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

2.0 Scope

All equipment or devices deployed in a DMZ owned and/or operated by University of Louisiana at Lafayette (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by University of Louisiana at Lafayette, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "University of Louisiana at Lafayette.com" domain or appears to be owned by University of Louisiana at Lafayette.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from Information Technology Security. All existing and future equipment deployed on University of Louisiana at Lafayette's un-trusted networks must comply with this policy.

3.0 Policy

3.1. Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by Information Technology Security for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the corporate wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of Information Technology Security upon demand, per the *Audit Policy*.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify compliance with this policy, Information Technology Security will periodically audit DMZ equipment per the *Audit Policy*.

3.2. General Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by Information Technology Security as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards [Insert a reference to any standards that you have]
- All patches/hot-fixes recommended by the equipment vendor and Information Technology Security must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by Information Technology Security.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by Information Technology Security) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to Information Technology Security-approved logs. Security-related events include (but are not limited to) the following:
    - User login failures.

    - Failure to obtain privileged access.
    - Access policy violations.
- Information Technology Security will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.3. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the *DMZ Equipment Deployment Process*.
- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- Information Technology Security must be invited to perform system/application audits prior to the deployment of new services.
- Information Technology Security must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.4. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	**Definitions**
DMZ (de-militarized zone)	Any un-trusted network connected to, but separated from, University of Louisiana at Lafayette's corporate network by a firewall, used for external (Internet/partner, etc.) access from within University of Louisiana at Lafayette, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.
Secure Channel	Out-of-band console management or channels using strong encryption according to the *Acceptable Encryption Policy*. Non-encrypted channels must use strong user authentication (one-time passwords).

Un-Trusted Network

Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

6.0 Revision History

Lab Anti-Virus Policy

1.0 Purpose

To establish requirements which must be met by all computers connected to University of Louisiana at Lafayette lab networks to ensure effective virus detection and prevention.

2.0 Scope

This policy applies to all University of Louisiana at Lafayette lab computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3.0 Policy

All University of Louisiana at Lafayette PC-based lab computers must have University of Louisiana at Lafayette's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into University of Louisiana at Lafayette's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Refer to University of Louisiana at Lafayette's *Anti-Virus Recommended Processes* to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time.

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of University of Louisiana at Lafayette's entire corporate network. As such, all University of Louisiana at Lafayette employees (including contractors and vendors with access to University of Louisiana at Lafayette systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University of Louisiana at Lafayette facility, has access to the University of Louisiana at Lafayette network, or stores any non-public University of Louisiana at Lafayette information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Information Technology Security administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at University of Louisiana at Lafayette. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "University of Louisiana at Lafayette", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for University of Louisiana at Lafayette accounts as for other non-University of Louisiana at Lafayette access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various University of Louisiana at Lafayette access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share University of Louisiana at Lafayette passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential University of Louisiana at Lafayette information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to Information Technology Security and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Information Technology Security or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the University of Louisiana at Lafayette Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to University of Louisiana at Lafayette's network from any host. These standards are designed to minimize the potential exposure to University of Louisiana at Lafayette from damages which may result from unauthorized use of University of Louisiana at Lafayette resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical University of Louisiana at Lafayette internal systems, etc.

2.0 Scope

This policy applies to all University of Louisiana at Lafayette employees, contractors, vendors and agents with a University of Louisiana at Lafayette-owned or personally-owned computer or workstation used to connect to the University of Louisiana at Lafayette network. This policy applies to remote access connections used to do work on behalf of University of Louisiana at Lafayette, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of University of Louisiana at Lafayette employees, contractors, vendors and agents with remote access privileges to University of Louisiana at Lafayette's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to University of Louisiana at Lafayette.
2. General access to the Internet for recreational use by immediate household members through the University of Louisiana at Lafayette Network on personal computers is permitted for employees that have flat-rate services. The University of Louisiana at Lafayette employee is responsible to ensure the family member does not violate any University of Louisiana at Lafayette policies, does not perform illegal activities, and does not use the access for outside business interests. The University of Louisiana at Lafayette employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of University of Louisiana at Lafayette's network:
   a. *Acceptable Encryption Policy*
   b. *Virtual Private Network (VPN) Policy*
   c. *Wireless Communications Policy*
   d. *Acceptable Use Policy*

4. For additional information regarding University of Louisiana at Lafayette's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any University of Louisiana at Lafayette employee provide their login or email password to anyone, not even family members.
3. University of Louisiana at Lafayette employees and contractors with remote access privileges must ensure that their University of Louisiana at Lafayette-owned or personal computer or workstation, which is remotely connected to University of Louisiana at Lafayette's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. University of Louisiana at Lafayette employees and contractors with remote access privileges to University of Louisiana at Lafayette's corporate network must not use non-University of Louisiana at Lafayette email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct University of Louisiana at Lafayette business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the University of Louisiana at Lafayette network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and Information Technology Security must approve security configurations for access to hardware.
9. All hosts that are connected to University of Louisiana at Lafayette internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to University of Louisiana at Lafayette's networks must meet the requirements of University of Louisiana at Lafayette-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the University of Louisiana at Lafayette production network must obtain prior approval from Remote Access Services and Information Technology Security.

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**

Cable Modem

Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP

Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem

A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing

Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a University of Louisiana at Lafayette-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into University of Louisiana at Lafayette and an ISP, depending on packet destination.

DSL

Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to he Internet).

Frame Relay

A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN

There are two flavors of Integrated Services Digital Network or SDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access

Any access to University of Louisiana at Lafayette's corporate network through a non-University of Louisiana at Lafayette controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-University of Louisiana at Lafayette network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into University of Louisiana at Lafayette's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Risk Assessment Policy

1.0 Purpose

To empower Information Technology Security to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope

Risk assessments can be conducted on any entity within University of Louisiana at Lafayette or any outside entity that has signed a *Third Party Agreement* with University of Louisiana at Lafayette. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs is the joint responsibility of Information Technology Security and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Information Technology Security Risk Assessment Team in the development of a remediation plan.

4.0 Risk Assessment Process

For additional information, go to the Risk Assessment Process.

5.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Entity	Any business unit, department, group, or third party, internal or external to University of Louisiana at Lafayette, responsible for maintaining University of Louisiana at Lafayette assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of University of Louisiana at Lafayette's key information assets and systems. Information Technology Security is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History

Router Security Policy

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of University of Louisiana at Lafayette.

2.0 Scope

All routers and switches connected to University of Louisiana at Lafayette production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
   a. IP directed broadcasts
   b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
   c. TCP small services
   d. UDP small services
   e. All source routing
   f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

   "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
Production Network	The "production network" is the network used in the daily business of University of Louisiana at Lafayette. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to University of Louisiana at Lafayette employees or impact their ability to do work.
Lab Network	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to University of Louisiana at Lafayette nor affect the production network.

6.0 Revision History

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by University of Louisiana at Lafayette. Effective implementation of this policy will minimize unauthorized access to University of Louisiana at Lafayette proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by University of Louisiana at Lafayette, and to servers registered under any University of Louisiana at Lafayette-owned internal network domain.

This policy is specifically for equipment on the internal University of Louisiana at Lafayette network. For secure configuration of equipment external to University of Louisiana at Lafayette on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at University of Louisiana at Lafayette must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Information Technology Security. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Information Technology Security.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved Information Technology Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to Information Technology Security, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within University of Louisiana at Lafayette.
- Audits will be managed by the internal audit group or Information Technology Security, in accordance with the *Audit Policy*. Information Technology Security will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
DMZ	De-militarized Zone. A network segment external to the corporate production network.

Server For purposes of this policy, a Server is defined as an internal University of Louisiana at Lafayette Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

THIRD PARTY CONNECTION AGREEMENT (TEMPLATE)

This Third Party Network Connection Agreement (the “Agreement”) by and between <Your Company Name>, a <Your Company’s State> corporation, with principal offices at <Your Address>, <Your Company’s State>, (“<Your Company>”) and ______________________ , a ________________ corporation, with principal offices at _____________________________ (“Company”), is entered into as of the date last written below (“the Effective Date”).

This Agreement consists of this signature page and the following attachments that are incorporated in this Agreement by this reference:

1. Attachment 1: Third Party Network Connection Agreement Terms and Conditions
2. Attachment 2 Network Connection Policy
3. Attachment 3: Third Party Connection Request - Information Requirements Document
4. Attachment 4: <Your Company> Non-Disclosure Agreement
5. Attachment 5: <Your Company> Equipment Loan Agreement

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by <Your Company’s State> law without regard to choice of law provisions.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

___________________ (“Company”)	<Your Company Name> (“<Your Company>”)
____________________ Authorized Signature	______________________________ Authorized Signature
____________________ Name	______________________________ Name
____________________ Date	______________________________ Date

THIRD PARTY CONNECTION AGREEMENT TERMS AND CONDITIONS

Object: To ensure that a secure method of connectivity is provided between <Your Company> and Company and to provide guidelines for the use of network and computing resources associated with the Network Connection as defined below.

Definition: "Network Connection" means one of the <Your Company> connectivity options listed in Section B of the Network Connection Policy.

1. Right to Use Network Connection. Company may only use the Network Connection for business purposes as outlined by the **Third Party Connection Request - Information Requirements Document**.

2. <Your Company>-Owned Equipment.

   2.1 <Your Company> may, in <Your Company> sole discretion, loan to Company certain equipment and/or software for use on Company premises (the <Your Company>-Owned Equipment) under the terms of the <Your Company> Equipment Loan Agreement set forth in Attachment 5. <Your Company>-Owned Equipment will only be configured for TCP/IP, and will be used solely by Company on Company's premises and for the purposes set forth in this Agreement.

   2.2 Company may modify the configuration of the <Your Company>-Owned Equipment only after notification and approval in writing by authorized <Your Company> personnel.

   2.3 Company will not change or delete any passwords set on <Your Company>-Owned Equipment without prior approval by authorized <Your Company> personnel. Promptly upon any such change, Company shall provide <Your Company> with such changed password.

3. Network Security.

   3.1 Company will allow only Company employees approved in advance by <Your Company> ("Authorized Company Employees") to access the Network Connection or any <Your Company>-Owned Equipment. Company shall be solely responsible for ensuring that Authorized Company Employees are not security risks, and upon <Your Company>'s request, Company will provide <Your Company> with any information reasonably necessary for <Your Company> to evaluate security issues relating to any Authorized Company Employee. Access to the Network Connection or any <Your Company>-Owned Equipment

3.2 Company will promptly notify <Your Company> whenever any Authorized Company Employee leaves Company's employ or no longer requires access to the Network Connection or <Your Company>-Owned Equipment.

3.3 Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the Network Connection (and Company's use of <Your Company>-Owned Equipment) is secure and is used only for authorized purposes, and (b) such party's business records and data are protected against improper access, use, loss alteration or destruction.

4. Notifications. Company shall notify <Your Company> in writing promptly upon a change in the user base for the work performed over the Network Connection or whenever in Company's opinion a change in the connection and/or functional requirements of the Network Connection is necessary.

5. Payment of Costs. Each party will be responsible for all costs incurred by that party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

6. DISCLAIMER OF WARRANTIES. NEITHER PARTY MAKES ANY WARRANTIES, EXPRESSED OR IMPLIED, CONCERNING ANY SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY. EXCEPT WITH RESPECT TO A PARTY'S CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM ANY DELAY, OMISSION OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF DATA PURSUANT TO THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, AND WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

8. Confidentiality. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the others technology and products that is confidential and of substantial value to that party, which value would be impaired if such information were disclosed to third parties ("Confidential Information"). Should

such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure. Each party agrees that it will not use in any way for its own account, except as provided herein, nor disclose to any third party, any such Confidential Information revealed to it by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information. Upon request by the receiving party, the disclosing party shall advise whether or not it considers any particular information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information. The receiving party's obligation of confidentiality shall not apply to information that: (a) is already known to the receiving party or is publicly available at the time of disclosure; (b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or (c) becomes publicly available after disclosure through no fault of the receiving party.

9. Term, Termination and Survival. This Agreement will remain in effect until terminated by either party. Either party may terminate this agreement for convenience by providing not less than thirty (30) days prior written notice, which notice will specify the effective date of termination. Either party may also terminate this Agreement immediately upon the other party's breach of this Agreement. Sections 5, 6, 7, 8, 10.1 and 10.2 shall survive any termination of this Agreement.

10. MISCELLANEOUS.

10.1 Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

10.2 Waiver. The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

10.3 Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.

10.4 Force Majeure. Neither party will be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

NETWORK CONNECTION POLICY (TEMPLATE)

Purpose: To ensure that a secure method of network connectivity between <Your Company> and all third parties and to provide a formalized method for the request, approval and tracking of such connections.

Scope: External company data network connections to <Your Company> can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the <Your Company> network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts. Therefore, all external company data network connections will be via the Global Partners Network. This policy applies to all new Third Party Network Connection requests and any existing Third Party Network Connections. When existing Third Party Network Connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed

Definitions: A "Network Connection" is defined as one of the connectivity options listed in Section B. below. “Third Parties” is defined as <Your Company> Partners, Vendors, Suppliers and the like.

A. Third-Party Connection Requests and Approvals

All requests for Third Party connections must be made using the appropriate method based on the support organization. [Add text about the specific support methods]

The required information is outlined in the **Third Party Connection Request - Information Requirements Document** (See Attachment 3 of this document). All information requested on this form must be completed prior to approval and sign off. It is Company’s responsibility to ensure that Company has provided all of the necessary information and that such information is correct.

All Third Party connection requests must have a <Your Company> VP level signature for approval. In some cases approval may be given at a lower level with pre-authorization from the appropriate <Your Company> VP. Also, all Third Parties requesting a Network Connection must complete and sign a <Your Company> Non-Disclosure Agreement.

As a part of the request and approval process, the technical and administrative contact within Company’s organization or someone at a higher level within Company will be required to read and sign the "Third Party Connection Agreement " and any additional documents, such as the <Your Company> Non-Disclosure Agreement.

B. Connectivity Options

The following five connectivity options are the standard methods of providing a Third Party Network Connection. Anything that deviates from these standard methods must have a waiver sign-off at the <Your Company> VP level.

1) Leased line (e.g. T1) - Leased lines for Third Parties will be terminated on the Partners network.

2) ISDN/FR - Dial leased lines will terminate on a Third Party only router located on the ECS or IT Partners network. Authentication for these connections must be as stated in Section E. below.

3) Encrypted Tunnel - Encrypted tunnels should[must?] be terminated on the Partners Network whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel on the dirty subnet, in which case the normal <Your Company> perimeter security measures will control access to Internal devices.

4) Telnet access from Internet - Telnet access from the Internet will be provided by first telneting to the Third Party gateway machine, where the connection will be authenticated per Section E. below. Once the connection is authenticated, telnet sessions to internal hosts will be limited to those services needed by using the authorization capabilities of <Your Company>Secure.

5) Remote Dial-up via PPP/SLIP - Remote dial-up via PPP/SLIP will be provided by a separate Third Party modem pool. The connection will be authenticated per Section E. below

C. Third Party (Partner) Access Points

When possible, Third Party (Partner) Access Points (PAPs should be established in locations such that the cost of the access is minimized. Each PAP should consist of at least one router with leased line with Frame Relay and/or ISDN capability.

D. Services Provided

In general, services provided over Third Party Network Connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. **Blanket access will not be provided for anyone.** The default policy position is to deny all access and then only allow those specific services that are needed and approved by <Your Company> pursuant to the established procedure.

In no case shall a Third Party Network Connection to <Your Company> be used as the Internet connection for the Third Party.

The standard set of allowable services are listed below:

File Exchange via ftp – Where possible, file exchange via ftp should take place on the existing <Your Company> ftp servers (ftp-eng.<Your Company>.com for engineering-related work or ftp.<Your Company>.com for all other work). IT supported Third Party connections have additional FTP services provided by a server in on the Partners Network.

Electronic Mail Exchange – Business-related email exchange between <Your Company> and Third Parties may be conducted over the Network Connection as needed. Mail from Third Party sites to non-<Your Company> addresses will not be allowed over the Network Connection.

Telnet Access – Telnet access will be provided to specific <Your Company> hosts, as needed. Employees from Third Parties will only be given accounts on the specific <Your Company> hosts that are needed. Where possible, router ACLs and static routes will be used to limit the paths of access to other internal <Your Company> hosts and devices. NOTE: NIS accounts and Directory Services are not to be established for employees of Third Parties who have accounts on <Your Company> hosts.

Web Resource Access – Access to internal web resources will be provided on an as-needed basis. Access will be provided by mirroring the appropriate web resources to a web server that resides on the Partners Network. Access to <Your Company>'s public web resources will be accomplished via the normal Internet access for the Third Party.

Access to Source Code Repositories This access will be decided on case by case basis.

Print Services – Print services can be provided to <Your Company> IT-supported Third Party connections by via two print spoolers on the <Your Company> Partners Network. <Your Company>-owned printers, that boot off the print spoolers will be located on the <Your Company> –extended network at the Third Party sites.

SQL*Net Access – This will be decided on a case by case basis.

ERP Access – This will be decided on a case by case basis.

NT File Exchange – File exchange will be provided by NT file servers located on the <Your Company> Partners Network. Each Third Party needing NT File exchange will be provided with a separate folder that is only accessible to that Party and the necessary people at <Your Company>.

E. Authentication for Third Party Network Connections

Third Party Network Connections made via remote dial-up using PPP/SLIP or standard telnet over the Internet will be authenticated using the Partners Authentication database and Token Access System. Currently, <Generic> is the token access system in use. A separate server will be established specifically for Third Parties. Reports showing who
has access via the tokens will be generated monthly and sent to the <Your Company> POCs for each Third Party for verification and review.

Telnet connection made via the Internet must be initiated to a separate which authenticates to the Partners Authentication database and Token Access System mentioned above..

ISDN/FR connections will be authenticated via the Partners <Your Company>Secure database, which is separate from the <Your Company> ISDN authentication database.

F. <Your Company> Equipment at Third Party Sites

In many cases it may be necessary to have <Your Company>-owned and maintained equipment at a Third Party site. All such equipment will be documented on the Third Party Connection Request – Information Requirements Document. Access to network devices such as routers and switches will only be provided to <Your Company> support personnel. All <Your Company>-Owned Equipment located at Third Party sites must be used only for business purposes. Any misuse of access or tampering with <Your Company>-provided hardware or software, except as authorized in writing by <Your Company>, may, in <Your Company>'s sole discretion, result in termination of the connection agreement with the Third Party. If <Your Company> equipment is loaned to a Third Party, the Third Party will be required to sign an appropriate <Your Company> Equipment Loan Agreement, if one is required

G. Protection of Company Private Information and Resources

The <Your Company> network support group responsible for the installation and configuration of a specific Third Party Connection must ensure that all possible measures have been taken to protect the integrity and privacy of <Your Company> confidential information. At no time should <Your Company> rely on access/authorization control mechanisms at the Third Party's site to protect or prohibit access to <Your Company> confidential information.

Security of Third Party Connections will be achieved by implementing "Access Control Lists" on the Partner Gateway routers to which the Third Party sites are connected. The ACLs will restrict access to pre-defined hosts within the internal <Your Company> network. The ACLs will be determined by the appropriate support organization. A set of default ACLs may be established as a baseline.

Enable-level access to <Your Company>-owned/maintained routers on Third Party premise will only be provided to the appropriate support organization. All other business personnel (i.e. Partner Site local technical support personnel) will have restricted access/read-only access to the routers at their site and will not be allowed to make configuration changes.

<Your Company> shall not have any responsibility for ensuring the protection of Third Party information. The Third Party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

H. Audit and Review of Third Party Network Connections

All aspects of Third Party Network Connections - up to, but not including Company's firewall, will be monitored by the appropriate <Your Company> network support group. Where possible, automated tools will be used to accomplish the auditing tasks. Monthly reports should be generated on the Partners Authentication database showing the specific login entries and the appropriate <Your Company> POC. Each <Your Company> Partner POC will receive a copy of the monthly reports showing all of the accounts pertaining to his/her area. Copies of the reports will also be mailed to the department directors.

Nightly audits will be performed on all <Your Company>-owned/maintained Third Party router/network device configurations and the output will be mailed to the appropriate <Your Company> network support group. Any unauthorized changes will be investigated immediately.

All Third Party Network Connections will be reviewed on a quarterly basis and information regarding specific Third Party Network Connection will be updated as necessary. Obsolete Third Party Network Connections will be terminated.

I. <Your Company> Corporate IT Information Security Organization

<Your Company> Corporate IT Information Security has the responsibility for maintaining related policies and standards. Corporate IT Information Security will also provide advice and assistance regarding judgment calls, and will facilitate information gathering in order to make a correct decision. Global coordination of confidentiality and non-disclosure agreements with all third parties is also the responsibility of <Your Company> Corporate IT Information Security.

J. <Your Company> Enterprise Network Services

The Enterprise Network Services Partners Group is responsible for all global firewall design, configuration and engineering required for support of the Global Partners Network.

THIRD PARTY CONNECTION REQUEST INFORMATION REQUIREMENTS DOCUMENT (TEMPLATE)

In accordance with the Network Connection Policy, all requests for Third Party Network Connections must be accompanied by this completed Information Requirements Document. This document should be completed by the <Your Company> person or group requesting the Network Connection.

A. Contact Information

Requester Information
Name:
Department Number:
Manager's Name:
Director's Name:
Phone Number:
Email Address:

Technical Contact Information
Name:
Department:
Manager's Name:
Director's Name:
Phone Number:
Pager Number:
Email Address

Back-up Point of Contact:
Name:
Department:
Manager's Name:
Director's Name:
Phone Number:
Pager Number:
Email Address

B. Problem Statement/Purpose of Connection
What is the desired end result? Company must include a statement about the business needs of the proposed connection.

C. Scope of Needs (In some cases, the scope of needs may be jointly determined by the supporting organization and the Third Party.)

What services are needed? (See Section D. of Network Connection Policy)
What are the privacy requirements (i.e. do you need encryption)?

What are the bandwidth needs?
How long is the connection needed?
Future requirements, if any.

D. Third Party Information

Third Party Name
Management contact (Name, Phone number, Email address)
Location (address) of termination point of the Network Connection (including building number, floor and room number)
Main phone number
Local Technical Support Hours (7X24, etc).
Escalation List
Host/domain names of the Third Party
Names (Email addresses, phone numbers) of all employees of the Third Party who will use this access. If not appropriate to list the names of all employees, then provide a count of the number of employees who will be using the connection.

E. What type of work will be done over the Network Connection?

What applications will be used?
What type of data transfers will be done?
How many files are involved?
What are the estimated hours of use each week? What are peek hours?

F. Are there any known issues such as special services that are required? Are there any unknown issues at this point, such as what internal <Your Company> services are needed?

G. Is a backup connection needed? (e.g., are there any critical business needs associated with this connection?)

H. What is the requested installation date? (Minimum lead-time is 60 days)

I. What is the approximate duration of the Third Party Network Connection?

J. Has a Non-Disclosure Agreement been sign with the Third Party or the appropriate employees of the Third Party?

K. Are there any exiting Network Connections at <Your Company> with this company?

L. Other useful information

Wireless Communication Policy

1.0 Purpose
This policy prohibits access to University of Louisiana at Lafayette networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Technology Security are approved for connectivity to University of Louisiana at Lafayette's networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of University of Louisiana at Lafayette's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to University of Louisiana at Lafayette’s networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards
All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Information Technology Security. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with Information Technology Security

3.2 Approved Technology
All wireless LAN access must use corporate-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication
All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History